المحاضرة التاسعة

أمن الأعمال الإلكترونية

E-business Security

أهداف المحاضرة

بنهاية المحاضرة يكون الطالب عنده:

1. استيعاب لأهمية أمن المعلومات في نجاح الأعمال الالكترونية
2. فهم أهم التهديدات والهجمات التي تواجه الأعمال الإلكترونية
3. القدرة على تقييم المخاطر المتعلقة ببنية الأعمال الإلكترونية
4. معرفة الوسائل الفنية اللازمة لحماية الأعمال الإلكترونية
5. معرفة وسائل الإدارية لحماية الأعمال الإلكترونية
6. بعض النصائح بخصوص أمن المعلومات والمواقع
7. القدرة على تقييم سياسات أمن المعلومات (من خلال سؤال المناقشة)

مقدمة

- **الأعمال الإلكترونية قد تكون تجارية إلكترونية أو عمليات داخلية أو حكومية أو غير هادفة للربح**
- **القراصنة اخترقوا نظم مكتب المباحث الفيدرالية الأمريكية المسؤولة عن فحص التاريخ الجنائي**
- **تم تسريب بيانات ٨٠ مليون زبون لشركة أنثيم Anthem الأمريكية**
- **بحث عن ٣٥٠ شركة من ١١ دولة وجد أن متوسط خسائرها ٣,٨ مليون دولار**
- **بلغت قيمة السرقات الالكترونية نحو مليار دولار وتم تسريب ٤٨٧ مليون سجل عام ٢٠١٥**
- **تلقت هيئة النصب والاحتيال الأمريكية ٢,٦ مليون بلاغ منها ٦٠% نصب و١٣ سرقة هوية**
- **خسائر البرامج الخبيثة بلغت ٤٩١ مليار دولار عام ٢٠١٤**
- **بعض الشركات أعلنت إفلاسها بسبب تسرب البيانات ومنها Nirvanix و Code Spaces**
- **تعرضت إسرائيل لهجوم الكتروني عام ٢٠١٣ شمل موقع الموساد والبورصة والبنك المركزي**
- **«سيأتى اليوم الذى لا تحترم خصوصية الأفراد الا أثناء النوم وأثناء الصلاة» Herbert Hoover**
- **سياسة الخصوصية للشركة غالباً ما تحتوى على نوع المعلومات التي تجمعها عنك وماذا تفعل بها، و الطرف الثالث الذى يحصل عليها وما هى إجراءات حماياتها، وكيفية إخبار الفرد عند تغييرها**

أهمية تأمين الأعمال الإلكترونية :

- الفشل في الحصول على ثقة الزبائن يقلل معدل التحول conversion rate
- الزبائن تريد أن تتأكد أن قوانين التجارة التقليدية تنطبق على قوانين التجارة الإلكترونية
- القراصنة متقدمين عن خبراء أمن المعلومات والمشرعين
- في الأعمال والتجارة الإلكترونية نتعامل مع شركات وعالم وأفراد بصورة افتراضية
- الخدمات والمنتجات الرقمية والمعلومات تعتبر أشياء غير ملموسة من الصعب اكتشاف سرقتها
- البرامج الخبيثة طالت شركات الكهرباء والمفاعلات النووية (مثل دودة ستاكسنت Stuxnet)
- البيانات والبرامج والخوادم والشبكات والأجهزة والخبراء هي أصول مهمة يجب حمايتها
- الزبائن تتردد في الشراء الالكتروني خوفا من الفيروسات وسرقة الهوية وسرقة المعلومات و
- هناك دراسة خلصت الى أنه إذا وثق الزبائن في الموقع سوف تزداد مشترياتهم بنسبة ٢٥%
- توقف الأعمال تعطل الموقع أو الخدمة وتسبب خسائر باهظة لشركات تعتمد على تقنية المعلومات
- تكاليف تسويات دعاوي انتهاك الخصوصية وحقوق الملكية الفكرية
- الخسائر الناجمة عن الكوارث الطبيعية أو الحرائق أو المرتبطة بالطقس

إدارة أمن المعلومات

إدارة أمن تكنولوجيا المعلومات: تخطيط وتصميم واختيار الأدوات والسياسات اللازمة لضمان سرية وسلامة وضمان الوصول الى المعلومات، والمساءلة، والموثوقية.

وتشمل مهام إدارة أمن تكنولوجيا المعلومات:

١. تحديد أهداف واستراتيجية وسياسة أمن المعلومات

٢. تحديد متطلبات أمن المعلومات من حيث السرية والسلامة وضمان الوصول والتوثيق

٣. تحديد التهديدات الأمنية للأصول وتحليلها
٤. تحديد وتحليل المخاطر (الخطر = احتمال حدوث التهديد x تكلفته)
٥. تحديد الأدوات والإجراءات والسياسات اللازمة لمواجهة هذه المخاطر
٦. تنفيذ وتشغيل هذه الأدوات
٧. صياغة وتنفيذ برنامج للتوعية الأمنية
٨. اكتشاف الحوادث والتعامل معها

ملفات الزبائن هي أصول تتعرض للفيروسات بنسبة معينة ويمكن حمايتها ببرامج مكافحة الفيروسات ويجب التوعية بشأنها

- **أمن المعلومات:** استخدام الأدوات اللازمة لحماية المعلومات من الوصول غير المصرح به، أو التسريب، أو التعديل، أو التدمير أو الاطلاع عليها

التهديدات والهجمات

الأصول: موارد لها قيمة وتكون ملموسة (المباني والأجهزة والأفراد) وغير ملموسة (البرامج والبيانات وسمعة الشركة وعلامتها التجارية)

- **أنواع التهديدات:**

1. **البرمجيات الخبيثة: مثل الفيروسات والديدان الخبيثة وأحصنة طروادة وذامبيى وبرامج الدعاية (تكافح بمضادات الفيروسات) والتجسس (سباي بوت Spybot) والنسخ الاحتياطي وبعض الوسائل الإدارية**

- **شبكة الروبوت Botnet: مجموعة من الحاسبات (عدادها بالآلاف) التي تم اختراقها والسيطرة عليها**

1. **تهديدات الطبيعة: تحدث بسبب الطبيعة مثل الزلازل والفيضانات و البراكين و الأعاصير وتؤدى الى إتلاف المباني والأنظمة (وسائل الحماية تشمل النسخ الاحتياطي والتأمين واختيار مكان مناسب)**

2. **تهديدات البيئة: مثل الحشرات والزواحف والقوارض والغبار وتسرب المياه**

3. **تهديدات بشرية: أخطاء المستخدمين (تنزيل ملف بدون فحص) ومدخلي البيانات والاداريين (عدم تطبيق سياسة أمن المعلومات) والموظفين الساخطين واللصوص والمخربين الذين يكسرون وسائل الحماية (تكافح بالتدريب والتوعية والقوانيين ووضع سياسات خاصة)**

٥. تهديدات صناعية: مثل التجسس الصناعي حيث توظف الشركات قراصنة للتجسس على المنافسين

التهديدات والهجمات

- **هجمات غير نشطة Passive Attack : فالمهاجم يحصل على معلومات دون تغيير أحد أصول الشركة، مثل التجسس أو معرفة العنوان البريدي لشخص وتحليل سلوكه على الإنترنت.**

  - **من الصعب اكتشافها ويجب التركيز على منعها عن طريق التشفير والتحكم في الوصول.**

- **هجمات نشطة Active Attack: يقوم المهاجم بتغيير أو تخريب أو تعطيل أحد الأصول (مثل الموقع الإلكتروني)، وانتحال الهوية (بطاقات الصراف، موقع إلكتروني، البريد الإلكتروني أو عنوان الانترنت) وإلغاء الملفات وتعطيل الأنظمة وتغيير الحسابات .**

- **هجمات داخلية: يقوم بها أفراد من داخل الشركة سواء كانت متعمدة أو غير متعمدة ومن الصعب منعها ويمكن الحد منها عن طريق التدريب والتوعية، والتحكم في الوصول (إعطاء الفرد الصلاحيات اللازمة فقط لتأدية عمله)**

- **هجمات خارجية: يقوم بها قراصنة ومخترقون وإرهابيون ومخربون من خارج المنظمة أو الدولة**

- **الهندسة الاجتماعية: أن يتصل بك شخص يدعى أنه موظف لبنك أو شركة ما للحصول علي معلومات سرية مثل كلمة المرور ورقم الحساب**

- **الثغرة Vulnerability: هي نقطة ضعف في النظام يمكن الهجوم من خلالها**

خدمات أمن المعلومات

الأعمال تحتاج الى خدمات (أو طلبات) معينة بخصوص أمن أصول تقنية المعلومات ومنها:

١- سرية المعلومات (Data Confidentially): حماية سرية المعلومات من الغير المصرح لهم مثل: منع كشف المعلومات الشخصية أو المالية لغير المصرح لهم

الخدمات الحكومية تحتاج الى سرية المعلومات

٢- سلامة المعلومات (Data Integrity) : هي منع غير المصرح لهم من تغيير أو تخريب المعلومات والأصول والتأكد من دقتها. مثل حماية بيانات المرتبات ودرجات الطلبة من التعديل

٣- ضمان الوصول (Availability): ضمان قدرة المستخدمين الشرعيين من الدخول على النظام ومنع المخترقين من الوصول الى النظام أو تخريب. مثل ضمان الوصول للبانر وبلاكبورد

٤- التوثيق: التحقق من شخصية الفرد أو الخادم أو الجهاز

٥- عدم الإنكار Non-repudiation: نظام يجعل الفرد لا يستطيع إنكار إرساله أو استقباله لمعاملة أو رسالة معينة. مثل عدم إنكار الشراء الالكتروني

وسائل أمن المعلومات

1. **وسائل مادية: الحراس والأسوار والأبواب والأقفال وطفاية الحريق، وأجهزة الإنذار، ومولد كهربائي احتياطي.**
2. **وسائل إدارية: مثل سياسة أمن المعلومات، سياسة الخصوصية، وخطة التعامل مع الكوارث، والنسخ الاحتياطية، والتوعية الأمنية والتدريب، وتدقيق أمن المعلومات**
3. **وسائل فنية: مثل التشفير، وسائل التوثيق، التحكم في الدخول، وسائل منع المخترقين، برامج مكافحة الفيروسات، والجدران النارية، وكاميرات المراقبة .**
4. **ضوابط قانونية وأخلاقية: مثل قوانين الخصوصية وقوانين الجرائم الالكترونية والقيم السائدة في المنظمة والمجتمع**

- **مقارنة الأدوات: من حيث السعر وإمكانياتها، والدعم الفني وتوافقها مع البرمجيات الأخرى. فعلى سبيل المثال، MacAfee, Norton برامج تجارية بينما AVG, AVAST مجانية**
- **النقطة الأضعف في أمن المعلومات هي الأفراد سواء كانوا زبائن أو موظفين**
- **مستوى أمن المعلومات هو مستوى أضعف نقطة لأن القراصنة تستغلها**

١. وسائل التوثيق Authentication

وسائل التوثيق: للتحقق من أصل رسالة معينة أو برنامج معين أو هوية المستخدم.

1. **مواصفات المستخدم: بصمة الأصبع، الحمض النووي، التوقيع، بصمة الصوت**

غير مقبولة من المجتمع وهى بطيئة ومكلفة وتحتاج الى أجهزة خاصة وقاعدة بيانات

الاسلوب	نوعها
شبكية العين	ثابتة
حدقة العين	ثابتة
شكل اليد	متغيرة
بصمة الاصبع	ثابتة
الحمض النووي	ثابت
التوقيع اليدوي	متغيرة

٢. أشياء يملكها: مثل بطاقة الهوية وبطاقة الصراف أو شريحة خاصة أو المفتاح.

- مكلفة بالمقارنة بكلمة المرور وقد تضيع أو تتلف أو تسرق

٣. أشياء يعرفها: مثل كلمة المرور، والرمز السرى أو إجابة سؤال معين.

- سياسة كلمة المرور: ينصح بتغييرها كل فترة وألا تقل عن ٨ حروف

وتشمل أرقام وحروف ورموز، وعدم استخدام كلمة مرور واحدة لأكثر من حساب،

وعدم كتابتها على ورقة.

- وسائل التوثيق تقدم خدمات أمن المعلومات الثلاثة: سرية وسلامة وضمان الوصول للمعلومات
- الشهادة الرقمية digital certificate هي محتوى رقمى ملحق فى صفحة الويب بهدف التحقق من هوية المرسل أو الخادم أو الحاسب الذى أرسل الرسالة.
- التوقيع الإلكتروني هو وسيلة إلكترونية للتحقق من هوية الشخص صاحب الرسالة أو المعاملة.

٢. التشفير (١)

الانترنت غير آمنة ولذلك يجب تشفير البيانات التي يرسلها الزبون أو الشركة كل منهما للآخر.

١. أشهر بروتوكول على الإطلاق يستخدم لتأمين التجارة الإلكترونية هو Secure Socket Layer (SSL)

متخصص في تأمين نقل البيانات بين متصفحي الانترنت ويقدم:

- تشفير الرسالة وتوفير سريتها
- حماية الرسالة من التغيير والتعديل
- توثيق شخصية المستخدمين عن طريق التوقيع الكتروني
- أهم استخداماته فى تأمين تجارة التجزئة B2C
- يوفر التوثيق، وسرية البيانات، وسلامتها، وعدم القدرة على الانكار

٢. التشفير (٢)

٢- IPsec وهو يستخدم في إنشاء VPN الشبكات الافتراضية الخاصة.

- فهو يوفر اتصال آمن بين نقطتين على الشبكة حيث يقوم بالتحقق من المستخدم وكذلك تشفير الرسالة
- كم أنه لا يسمح بأي نوع من الفلاتر بين النقطتين المتصلتين بمعنى أنه لا يمكن استخدامه مع وجود جدران النار في طريقه.
- وغالبا ما يستخدم في الحالات التالية:
  - لتأمين المعاملات بين المؤسسات المالية

- ويستخدم في تأمين تجارة الأعمال B2B
- في تأمين المعاملات بين المؤسسة وفروعها.
- بين أجهزة العاملين والزبائن والموردين

٣. أنظمة اكتشاف المخترقين

- **هي أنظمة وبرامج لكشف المتسللين الغير مصرح لهم بالدخول**

أهم وسائل إكتشاف المخترقين:

- **Log files ملف تسجيل الأنشطة: هو ملف يسجل كل الأنشطة التي تتم من خلال نظام التشغيل**
- **Audit Trail ملفات المراجعة والتدقيق: هي ملفات تحفظ بيانات عن التغييرات التي يجريها المستخدمون في الملفات والبرامج بما فيها تفاصيل التغيير واسم المستخدم وتاريخ ووقت التغيير. تعتبر افضل طريقة لاكتشاف تلاعب الموظفين المصرح لهم بالعمل على هذه النظم**
- **آنية العسل Honey-pots : يتم استخدام بعض الحيل والخدع لاستدراج الدخلاء مثل أن يضع ملف باسم "كلمات السر" في مكان مخفي على السيرفر لكن يمكن الوصول اليه وبالتالي يتم تسجيل عناويين IP من يحاول سحب نسخة من هذا الملف سواء من الموظفين أو من الخارج وبالتالي يتم مراقبتهم.**
- **أجهزة الإنذار وكاميرات المراقبة**

١. سياسة أمن المعلومات

- **سياسة أمن المعلومات: بيان رسمي يحدد قواعد وإجراءات وأدوات لحماية أصول المنظمة ومسؤوليات الأفراد، وما يجب حمايته ولماذا، ويحدد السلوك المقبول ومعلومات الاتصال.**
- **ويجب إشراك المدراء وأخصائي نظم المعلومات والمستخدمين والقانونيين والإدارة العليا**
- **مراحل تصميمها: تحليل المخاطر، صياغة السياسة، الموافقة عليها، التوعية، تنفيذها، تقييمها**
- **محتوياتها: الأمن المادي، جلب الموظفين والاستغناء عنهم، حماية البيانات، أمن الاتصالات، أمن الأجهزة والبرمجيات، الدعم الفني، الخصوصية، الوصول للنظم، المساءلة والعقوبات، الإبلاغ عن الانتهاكات**
- **سياسة الاستغناء عن الموظفين: إزالة اسمه من قائمة المصرح لهم بالوصول، وإبلاغ الحرس والأطراف الأخرى، إلغاء حساباتهم، استعادة الأصول منهم**
- **سياسة النسخ الاحتياطية: تحدث دورياً، وتشفر، وتخزن بعيدا عن موقع العمل، ويتم إختبارها**
- **سياسة الجدار الناري: التأكد من أنه يعمل، غلق النوافذ الغير مستخدمة، منع المواقع المشبوهة، حمايته بمضاد للفيروسات، وتخصيص جهاز له، واستخدام جدار ناري للحاسبات والخوادم والشبكة**
- **سياسة الانترنت: تستخدم فقط لأغراض العمل، عدم زيارة مواقع مشبوهة، استخدام شخصي معقول**

تحديد التهديدات الأمنية للأصول وتحليلها

الأصل	التهديد	وسائل الحماية	احتمال حدوثه	العواقب	المستوى	الأولوية
الموجه	هجمات قراصنة	وسائل منع المخترقين	محتمل	متوسطة	مرتفع	١
الخادم	حرائق	خطة التعامل مع الكوارث	غير محتمل	عالية	مرتفع	٢
الانترنت الأرضي	انقطاع الوصلة	شبكة واي فاي	غير محتمل	عالية	مرتفع	٢
الخبراء	ترك العمل	إعداد بدائل	محتمل	عالية	متوسط	١

- **طريقة البدائية:** إتباع المعايير والإجراءات وأفضل الممارسات المتبعة في الصناعات المماثلة
- **الطريقة الغير رسمية:** تتم بواسطة المتخصصين والخبراء داخل المؤسسة
- **الطريقة الرسمية:** الاستعانة بشركات متخصصة في هذا المجال

٢. خطة استمرارية الأعمال والتعافي من الكوارث

الكارثة: هي حدث غير متوقع قد يعطل الأنظمة والخدمات أو يدمر الأصول والأجهزة ويكون له تأثير طويل المدى على المؤسسة.

مثل تعطل الموقع، زلزال يدمر المنشأة، فقدان ملف مهم، حريق، ديدان خبيثة، انقطاع الكهرباء

خطة استمرارية الأعمال: هي خطة تحدد الأنظمة والإجراءات والاحتياطات اللازمة لمنع الكوارث المختلفة والتعامل معها والتعافي منها سواء كانت طبيعية أو بشرية أو متعلقة بالبرمجيات الخبيثة.

مراحلها كالآتي:

1. **تكوين الفريق المسؤول عن التخطيط والتنفيذ**
2. **تقييم المخاطر ووضع الأولويات للأصول الواجب**
3. **وضع استراتيجيات لاستمرارية الوظائف الحرجة**
4. **شراء وتخزين الأدوات المطلوبة ومراجعة الخطة**
5. **وضع معايير وإجراءات لضمان نجاح الخطة**
6. **تنفيذ الخطة عن حدوث الكارثة**

التعافي من كارثة فقدان ملف مهم يتطلب نسخة احتياطية منه، والتعامل مع الحريق يتطلب طفاية حريق ورقم هاتف إدارة الدفاع المدني أما التعافي من الحريق فيتطلب التأمين على المباني والأجهزة.

سؤال: ما هي خطة التعامل مع الفيضانات وانقطاع الكهرباء؟

خصائص خاصة بالموقع الإلكتروني

- **يستخدم نظام لقياس السمعة reputation system كما هو متبع في eBay حيث تزداد نسبة الثقة كلما قلت الشكاوى ضد الشخص أو الشركة**





- عليه اللوجو والعلامة التجارية والرابط URL الخاص بالشركة
- من السهل تصفح الموقع وجودة الصور والمحتوى وتناسق الألوان
- يوفر معلومات اتصال وإرشادات وأسئلة شائعة
- يوفر عروض خاصة
- يوفر خدمة التسجيل في الموقع
- يضع علامة الهيئة التي تعتمد أمن المعلومات لموقعك
- يستخدم تكنولوجيا حديثة وسرعة استجابة الموقع
- يوضح ويشرح سياسة الخصوصية
- يشفر المعلومات باستخدام بروتوكول https وعليه صورة القفل، لكن هذا البروتوكول بطيء

نصائح خاصة بأمن المعلومات

١- استخدم البطاقة الائتمانية التي يتم شحنها بقيمة المشتريات.

٢- استخدم الجهاز الخاص بك وتجنب الشبكات العامة خاصة شبكات اللاسلكي.

٣- حدث برامج مكافحة الفيروسات باستمرار

٤- تجنب فتح الرسائل الالكترونية من المجهولين والدخول إلى الروابط الموجودة فيها.

٥- احرص على التعامل مع المواقع الإلكترونية المشهورة والمعروفة.

٦- تابع مصروفاتك ومراجعة حساباتك البنكية بصورة دورية

٧- تجنب نشر معلومات شخصية على مواقع التواصل الاجتماعي

٨- افحص الملفات ضد الفيروسات قبل تنزيلها

٩- تجنب البرامج الغير أصلية ولا تنزل البرامج الا من مواقعها الأصلية

١٠- تأكد من وجود نسخ احتياطية من الملفات والبرامج المهمة

دوافع القراصنة

- القراصنة: هم أشخاص يخترقون أنظمة الحاسوب مستغلين ثغرات معينة
- دوافع القراصنة:

➢ التجسس الصناعي: بعض الشركات تؤجر القراصنة لسرقة أسرار الشركات المنافسة

➢ الدفاع عن الدولة: بعض الدول كونت جيوشاً من القراصنة للدفاع عن بنيتها الالكترونية أو لمهاجمة دول أخرى (السيطرة على البحر ثم الجو ثم الفضاء الإلكتروني)

➢ للتعلم والتحدى: لتحدى شركة أو هيئة معينة أو للمتعة وإثبات الذات و تجربة فكرة معينة

- **أسباب أخلاقية: تؤجره الشركات لاختراق النظام لاكتشاف أماكن الضعف فيه**
- **السرقة: سرقة هوية الأفراد وأموالهم**
- **الإرهاب: دوافعهم التعصب الدين أو المذهب**
- **الثأر: الثأر من شخص أو شركة أو دولة**

1. **«من يسيطر على البحر يسيطر على العالم»**
2. **«من يسيطر على الفضاء يسيطر على العالم»**
3. **«من يسيطر على الفضاء الالكترونى يسيطر على العالم»**

نهاية المحاضره التاسعه بعد التعديل

محتوى المحاضره فقط

اختكم ميييووش٢